

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Philip Alan Drechsler,

Defendant(s)

Case No. 2:23-mj-01874

<p align="center">FILED CLERK, U.S. DISTRICT COURT</p> <p align="center">4/18/2023</p> <p align="center">CENTRAL DISTRICT OF CALIFORNIA</p> <p align="center">BY: <u>jm</u> DEPUTY</p>

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 17, 2020 through June 28, 2021, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section

18 U.S.C. § 2252A(a)(2)(B)
18 U.S.C. § 2252A(a)(5)(B)

Offense Description

Distribution of child pornography
Possession of and access with intent to
view child pornography

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Chelsea Malone

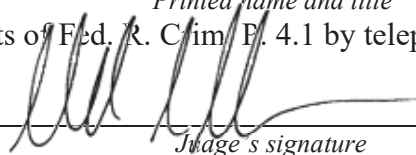
Complainant's signature

Chelsea Malone, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 4/18/2023


Judge's signature

City and state: Los Angeles, California

Hon. Michael Wilner, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Chelsea Malone, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Philip Alan Drechsler ("DRECHSLER", or "SUBJECT PERSON"), date of birth July 5, 1962, for violations of 18 U.S.C. §§ 2252A(a)(2)(B) (distribution of child pornography) and §§ 2252A(a)(5)(B) (possession of and access with intent to view child pornography).

2. The facts set forth in this affidavit are based upon information provided by other U.S. law enforcement agents; written reports about this investigation that I have received from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts; and my personal observations, training, experience, and background as a Special Agent. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF SPECIAL AGENT CHELSEA MALONE

3. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since April 2022. One of my responsibilities with the FBI includes

investigations into the sexual exploitation of children and child pornography in the Central District of California, in violation of 18 U.S.C. §§ 2251, among other violations. I have received training in the investigation and prosecution of child pornography and child exploitation offenses. Through my training and experience, I have become familiar with the methods used by people who commit offenses involving the sexual exploitation of children. My training and experience have given me an understanding of how people who commit offenses relating to the sexual exploitation of children use the Internet to facilitate and commit those offenses. I make this affidavit based upon my personal knowledge and experience, my review of pertinent documentation, my consultation and confirmation with more experienced agents in this violation, and discussions with other law enforcement officers.

III. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

4. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

5. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child

pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital

device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address - IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination

of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer

image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

vi. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include

encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

x. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

xi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xiv. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

xii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xiii. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xiv. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xv. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

xvi. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

IV. SUMMARY OF PROBABLE CAUSE

6. As set forth in greater detail below, DRECHSLER, using the alias "Karen Flores," was a member of an online community of individuals who regularly sent and received child pornography via a group chat within the Telegram application called "The Playground Lives." Specifically, there is probable cause to believe DRECHSLER knowingly accessed with intent to view and distributed child pornography within "The Playground Lives" chat between approximately August 17, 2020, and June 28, 2021. There is also probable cause to believe DRECHSLER distributed child pornography in that chat between approximately

August 17, 2020, and June 28, 2021. After reviewing the files DRECHSLER shared in the chat, I determined approximately 125 were suspected CSAM.

7. FBI executed federal search warrants on April 6, 2023 of DRECHSLER's home and person. During the search, I previewed DRECHSLER's personal cellphone, an iPhone 11 with the serial number C6KCZDQGN7ZQ. On it, I found what appeared to be CSAM videos in the "recently deleted" photo album folder. I also found the Telegram application and evidence that the account DRECHSLER used to access "The Playground Lives" chat may have been had been deleted. The email address phil.ir818@gmail.com, which was, as described below, used to create the telephone number connected to "The Playground Lives" chat, was still connected to the device and accessible through the email application.

8. On April 17, 2023, I interviewed M.D. – the spouse of DRECHSLER – who stated that a few days ago, DRECHSLER made concerning statements about taking his own life and then had driven to Cincinnati, Ohio with three firearms. DRECHSLER has one firearm registered to him; however, two additional firearms were found during the search warrant that were not registered to DRECHSLER. It is unknown how DRECHSLER obtained these weapons, nor if he possesses any additional unregistered weapons.

V. STATEMENT OF PROBABLE CAUSE

9. The investigation into DRECHSLER's use of the Telegram group chat known as "The Playground Lives" to access and distribute child sexual abuse material ("CSAM") was predicated on an investigation that began in the FBI Office in Kansas City, Missouri. I have consulted with the investigators

and reviewed evidence they have collected and learned the following facts establishing probable cause to believe that the SUBJECT PERSON committed the SUBJECT OFFENSES and evidence of and relating to the SUBJECT OFFENSES was found at the SUBJECT PREMISES.

**A. A Prior Child Exploitation Investigation Leads to the
Discovery of DRECHSLER's Involvement in The Playground
Lives Chat**

10. On or about June 16th, 2021, FBI Task Force Officer ("TFO") David Albers interviewed Joshua Goodspeed ("Goodspeed"), the subject of a separate child pornography investigation. During that interview, Goodspeed signed a Consent to Assume Online Presence form, in which he voluntarily authorized TFO Albers to take over control and use the online presence of his Telegram account associated with Goodspeed's email, rockyrockhopper0517@gmail.com. The consent included the access of stored information and use and disclosure of communications. TFO Albers identified a Telegram group chat called "The Playground Lives", which was created on August 10, 2020, and had at the time had 23 group members. At the time of initial identification, the group chat involved approximately 1,683 photos, 8,128 videos, and 36 links to shared files, all of which depicted suspected CSAM and included primarily prepubescent females, some as young as toddler age, involved in sexually explicit activity.

11. On or about July 6, 2021, TFO Albers observed a user with the screenname "Karen Flores" within "The Playground Lives" group chat. In order to create a Telegram account, a telephone number is needed. When a username is clicked on in the Telegram

application, the telephone number associated with the account may be displayed. "Karen Flores", who was subsequently identified as DRECHSLER, as described below, publicly displayed the telephone number 424-259-1545 (the "424" Phone Number") as associated with the account. Between approximately August 17th, 2020, and June 28th, 2021, DRECHSLER, under the screen name Karen Flores, shared approximately 117 suspected CSAM videos in "The Playground Lives."

12. TFO Albers next determined that the 424 Phone Number was registered through Google.

13. On or about July 7, 2021, an administrative subpoena was served by Detective Albers to Google for the subscriber data and IP logs associated with the 424 Phone Number.

14. On or about August 10th, 2021, Google provided a response to TFO Albers who reviewed the response and learned the following:

a. The 424 Phone Number was created on April 21, 2021, with the IP address 191.96.121.166 and was registered to Phil Irwin, email address phil.ir818@gmail.com. 818 is the area code for the San Fernando Valley, a city approximately 10 miles south of Santa Clarita.

b. Several IP addresses were used to access the Google account (phil.ir818@gmail.com); however, queries through the American Registry for Internet Numbers ("AIRN") yielded that all but one IP address resolved to Virtual Private Networks ("VPNs"). The one IP address that was not registered

to a VPN, IP address 172.91.217.214, was used to access the Google account (phil.ir818@gmail.com) on May 16, 2021.¹

c. A subsequent AIRN query yielded that IP address 172.91.217.214 was registered through Charter Communications.

d. On or about August 10th, 2021, TFO Albers served an administrative subpoena to Charter Communications to disclose the subscriber information for the IP address 172.91.217.214. Charter Communications provided the following account information about the account holder:

- i. Name: PHILIP DRECHSLER
- ii. Address: [DRECHSLER's home address removed]
- iii. Email: pdrechsler99@gmail.com
- iv. Phone: [Ending in -7756]
- v. Start date: September 13th, 2020, and active to the date of the subpoena.

B. FBI Lancaster's Investigation of DRECHSLER Reveals DRECHSLER was a Frequent Contributor to "The Playground Lives" Chat, Including Repeatedly Distributing CSAM of Young Children

¹VPNs create a secure and encrypted connection between the internet and the device being used to access the internet. VPNs allow someone to stay private online and can obscure their identity. Some VPNs are set up to auto-connect, while some require manual connection. The prior use of a VPN indicates that either a VPN was not used when accessing the 424 Phone Number account during that specific instance or a VPN was used, but the connection was dropped.

15. The FBI Los Angeles Lancaster Resident Agency ("FBI Lancaster") opened an investigation regarding DRECHSLER's use of the Telegram group chat "The Playground Lives" to access and distribute CSAM.

16. On or about August 31, 2022, I was assigned to the investigation.

17. On or about December 20, 2022, I received the exported chat log from "The Playground Lives" group chat from TFO Albers.

18. During my investigation, I observed that DRECHSLER interacted within "The Playground Lives" approximately 145 times throughout August 17, 2020 through June 28, 2021. Of the 145 interactions, DRECHSLER shared 117 videos, 9 images, 2 gifs and 1 link to shared file(s) and commented about 16 times. I could not access the file sharing link due to its removal from the hosting platform for "gross violation of Mega's terms of service."² Of the shared files, I observed that approximately 125 were suspected CSAM.

19. A detailed description of some of DRECHSLER's contributions to the chat follow:

² Mega.nz ("Mega") is a cloud-based storage and file hosting website based in New Zealand. Anyone can create a Mega account with just an email and password. Once an account is created, users can access up to 15 gigabytes of digital storage for free. The users of a Mega account can share files to the users account by creating a hyperlink to folders and specific files within the users account. File are encrypted via end-to-end encryption, which means Mega does not have access to the files and only the user can see or share the files. Based on these facts and my training and experience, I know that Mega files are often used to host and send CSAM.

a. Images & Videos:

i. On or about January 31, 2021, DRECHSLER commented "Facecast³. . . follow & tip" and shared three videos and an image of what appears to be a prepubescent or early pubescent female. These videos appear to be of the same girl being orally penetrated by the penis of who appears to be an adult male. The aforementioned photo appears to be of the same girl as in the videos and has a Facecast ID number on the top right of the image.

ii. On or about March 13, 2021, DRECHSLER posted two videos titled "Georgia papa fingering.mp4" and "Georgia peach." The videos depicted what appeared to be the same prepubescent or early pubescent girl laying naked with her buttock, breasts, and vagina exposed at various points in the videos. The hand of what appears to be an adult male touches the girl's breasts and vagina. One of these videos depicts the girl being vaginally penetrated by the fingers on the male.

iii. On or about September 4, 2021, DRECHSLER shared an approximately 17 minute and 40 second video that compiled approximately nine different videos. Of those videos, one depicted what appeared to be a male infant or toddler laying down with what appeared to be adult female performing oral sex on the toddler. In another video within the compilation, what appears to be the same male was lying on his back with a pre-pubescent girl on top of him and his penis inserted into her vagina. The same adult female appeared to be

³ Based on my training and experience, I know Facecast is an online video chatting service that is commonly used for the sexual exploitation of children.

instructing the girl on how to have sex with the toddler while she was filming it.

iv. On or about June 5, 2021, DRECHSLER shared a video of what appears to be pre-pubescent girl being orally penetrated by the penis of an adult male.

v. On or about June 15, 2021, DRECHSLER shared a video of what appears to be two pre-pubescent girls exposing their breasts and vagina.

b. Comments:

i. DRECHSLER commented approximately 16 times. Based on my training and experience, I believe some of comments made by DRECHSLER indicate he is a member of other unknown group chats involved in the exchange of child sexual abuse material, as well as the intent to deceive or evade law enforcement officers. One example of a comment that DRECHSLER is as follows:

ii. On or around March 22, 2021, DRECHSLER commented, "She is worth it! How do you get such a clean cap⁴?" in response to a suspected CSAM video posted by another user within the group chat. The user, whose account has since been deleted, responded "I use m3u8 downloader".⁵ DRECHSLER responded "Thx!"

⁴ Based on my training and experience, I know that "cap" is often a shorthand for "capture" meaning screen capture or screen recording.

⁵ An M3U8 downloader is used to download videos that are live-streamed. Based on my training and experience, I know that most live stream videos are not available for download but using an M3U8 downloader would allow a user to download a streamed video. Furthermore, I know that individuals are able to manufacture child pornography through livestream platforms by

**C. DRECHSLER is the User and Owner of the Above-Mentioned
IP Address, Email Address, Phone Number, and Residence
Used to Facilitate the SUBJECT OFFENSES**

20. Based on the information provided by Google and Charter Communications, as well as my investigation to date, I believe there is probable cause "Karen Flores" and "Phil Irwin" are aliases used by DRECHSLER to obscure his identity to facilitate him distributing, possessing, and accessing with intent to view CSAM.

a. As previously outlined, Charter Communications provided that IP address 172.91.217.214 was registered to Philip Drechsler, [DRECHSLER's home address] (The "SUBJECT PREMISES").

b. On March 7, 2023, I submitted an administrative subpoena to Google LLC for phil.ir818@gmail.com.

c. On March 8, 2023, I received the subscriber information from Google, which confirmed that the last login for the email account phil.ir818@gmail.com was on February 27, 2023. The recovery phone number is listed as 424-259-1545, which is the "424 Phone Number" publicly listed as "Karen Flores" within the Telegram chat room "The Playground Lives." Between July 2022 and February 2023, IP address 172.91.217.214 was used to log into the Google account phil.ir818@gmail.com approximately 11 times.

recording children engaged in sexual activity or in sexually suggestive poses.

D. During the Execution of the Search Warrants, I Found What Appeared to be CSAM in DRECHSLER's cellphone and DRECHSLER Admitted to Knowing the Content Was on His Device and That Some of the Content Depicted Children.

21. On March 29, 2023, the Honorable Alexander F. MacKinnon of the United States District Court in the Central District of California issued federal search warrants 2:23-MJ-1466 and 2:23-MJ-1467 for DRECHSLER's residence and DRECHSLER's person respectively.

22. On April 6, 2023, FBI executed the search warrants. Information learned as the result of those search warrant follows:

a. During the course of the search operation, I interviewed DRECHSLER. During the time, I also previewed his personal cellphone for evidence and found the following:

- i. Within the "Recently Deleted" Folder in Photos Application, I observed suspected CSAM, which I showed DRECHSLER.
- ii. Within the Telegram application, I observed several group chats, but I did not see "The Playground Lives" chat.

23. DRECHSLER stated that he recognized the content in the folder. Amongst other videos, I showed DRECHSLER four videos of what appears to be pre-pubescent girls with exposed chests from within the captioned folder. I also showed DRECHSLER a video of a pre-pubescent girl lifting her leg in the air, which exposed her genitalia. DRECHSLER stated that he could not tell the age of the individuals and did not think it was child pornography. I asked him if the individuals looked like

adults or children and DRECHSLER confirmed that they looked like children.

24. DRECHSLER admitted to accessing some of the videos I showed him, which appeared to be CSAM, on publicly available platforms. Specifically, the videos appeared to have been downloaded from Tiktok.

F. DRECHSLER Expressed Suicidal Ideation and Then Fled to Ohio with Guns

25. On April 17, 2023, I interviewed DRECHSLER'S wife, M.D., to obtain additional information regarding DRECHSLER. M.D. stated that DRECHSLER left California and drove to Ohio last week. DRECHSLER took his shotgun and two pistols with him. M.D. stated that DRECHSLER left the majority of his belongings behind and told M.D. to donate them. DRECHSLER told M.D. that he did not intend to return home. DRECHSLER made statements that he wanted to say goodbye to his daughter in Ohio and see his parents' gravesite one final time. DRECHSLER stated that he had nothing to live for and that he wanted to kill himself. M.D. stated that M.D. does not believe DRECHSLER would harm himself or anyone else in Cincinnati, Ohio, but if DRECHSLER were to do so, it would be in Toledo, Ohio where his parents' gravesite is located. M.D. provided the location of the hotel where DRECHSLER is residing, as described below, as well as the address of the gravesite.

26. On April 17, 2023, at my direction, Special Agents and Task Force Officers in Cincinnati, Ohio conducted surveillance at the hotel where DRECHSLER was residing, the Wingate by Wyndham hotel located at 4320 Glendale Milford Road Cincinnati, Ohio 45242. DRECHSLER's vehicle, a grey Honda

Accord California license plate 7BPG234, was observed in the parking lot of the hotel. A prior query to the California Department of Motor Vehicles on or about January 11, 2023, confirmed the vehicle is registered to DRECHSLER. Officers confirmed with the hotel staff that DRECHSLER checked into the Wingate hotel and was scheduled to check out on April 20, 2023. M.D. believes that once DRECHSLER checks out of the hotel and departs Cincinnati, he will likely travel to Toledo.

27. In addition to the above, on April 18, 2023, a special agent with FBI in Cincinnati informed me that law enforcement personnel who were conducting surveillance of the Wingate hotel spoke with the hotel manager, who informed the officers that a group of high school students on a field trip were expected to be checking into the hotel on April 19, 2023 at a time unknown.

VII. CONCLUSION

28. For all the reasons described above, there is probable cause for the requested complaint and arrest warrant against Philip Alan Drechsler for violations of 18 U.S.C. § 2252A(a)(2)(B) (distribution of child pornography) and § 2252A(a)(5)(B) (possession of and access with intent to view child pornography).